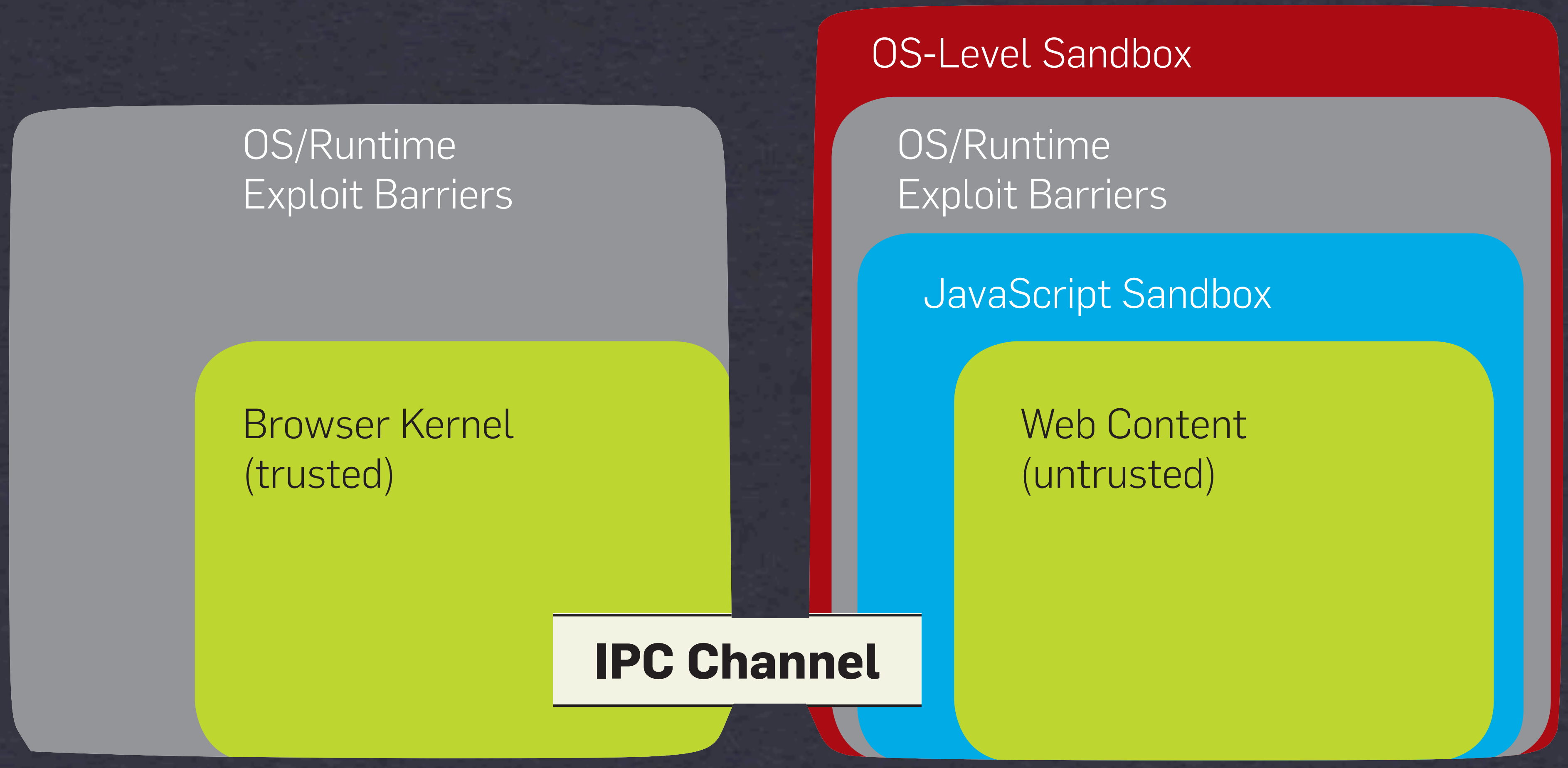
Material and some slide content from:
Taylor et. al.
http://queue.acm.org/detail.cfm?id=1556050



Architecture in Practice: Chrome

Reid Holmes

NFP: Security

- Security: "The protection afforded a system to preserve its integrity, availability, and confidentiality if its resources."
- Confidentiality
  - Preserving the **confidentiality** of information means preventing unauthorized parties from accessing the information or perhaps even being aware of the existence of the information. I.e., secrecy.
- Integrity
  - Maintaining the **integrity** of information means that only authorized parties can manipulate the information and do so only in authorized ways.
- Availability
  - Resources are **available** if they are accessible by authorized parties on all appropriate occasions.

Security principles

- Security is a cross-cutting concern that cannot be retroactively added to a system.
- Several principles exist for reasoning about design decisions from a security perspective:
  - Least privilege
  - Fail-safe defaults
  - Economy of mechanism
  - Open design
  - Separation of privilege
  - Least common mechanism
  - Psychological acceptability
  - Defense in depth

Chrome

- Online content is insecure and can compromise:
  - Confidentiality: Leak user data
  - Integrity: Read/write arbitrary data on disk
  - Availability: Crash host application and/or OS

Chrome relies on **least privilege, separation of privilege,** and **defense in depth** to securely parse and render insecure content.

Chrome architecture